REMARKS

Claims 1-27 are currently pending in the application. By this amendment, claims 1, 4-9, 14, 15, 17-18, and 25 are amended for the Examiner's consideration. The foregoing separate sheets marked as "Listing of Claims" shows all the claims in the application, with an indication of the current status of each .

In the specification, the paragraph beginning at page 12, line 6 has been amended to correct a spelling error and supply missing reference information. No new matter has been added.

The Examiner has objected to an informality in the specification, namely, a missing U.S. Patent Application serial number at page 12, line 14. This number has been supplied by the foregoing amendment.

The Examiner has also objected to certain informalities in the specification and claims, and has made a 35 U.S.C. §112, second paragraph, rejection of claims 4-9 and 15-17. The claims have been amended to overcome these objections and rejections.

The Examiner has rejected claims 1-9 and 11-27 under 35 U.S.C. §103(a) as being unpatentable over EP 0 908 810 A2 to Candelore et al. ("Candelore") in view of U.S. Patent No. 5,619,571 to Sandstrom et al. ("Sandstrom"). Claim 10 is rejected under 35 U.S.C. §103(a) as being unpatentable over Candelore in view of Sandstrom and further in view of U.S. Patent No. 5,745,643 to Mishina.

Candelore discloses an apparatus for efficiently and securely transferring blocks of program information between a secure circuit and an external storage device, where the program information is communicated in block chains for more robust encryption and to reduce authentication data overhead (col 1, lines 5-11). In this respect the disclosure is within the prior art as described in the background of the present invention. In Candelore, there is provision for encryption and authentication of block chains. In one embodiment, there is encryption with authentication being optional (col 1, lines 12-14); in another embodiment, there is authentication with encryption being optional (col 1, lines 15-17). But in this context both encryption and authentication refer to the basic program material being transmitted. Candelore discusses keys in connection with the encryption of program material, which is within the prior art (see col 4, lines 27-51 and col 11, lines 20-37). Candelore also provides for reordering of blocks to enhance security (col 1, lines 20-22), and for dependence of encryption keys upon a key that is unique to each decoder unit (col 31, lines 12-14 and lines 23-34).

The present invention is directed to the protection of movies and other programming transmitted to a mass storage device on a set-top-box (STB). The context for the invention is existing digital audio and video transmission and reception standards and STB architectures, and an object of the invention is to provide an encryption technique that is compatible with this context (page 6, lines 3-5). It is also an object of the invention to provide an encryption technique that allows reduced data manipulation using a single key or a limited number of keys that can be securely handled in a simple manner, allowing playback on an authorized STB while preventing playback on different devices (page 6, lines 3-12). The technique of the invention provides for key usage in three particulars: defining a write order of data blocks to non-sequential storage locations in the mass storage device; allocating corresponding sectors in a file allocation table; and encrypting the file allocation table. Significantly, there is no need to authenticate a user, since the keys may be maintained internal to the decoder (page 7, lines 20-27). While Candelore acknowledges the importance of dependence upon a key unique to each decoder unit, that is in reference to the encryption of the programming material. There is no suggestion in Candelore of a connection between block re-ordering and a key maintained internal to the decoder, or unique to the decoder (page 13, lines 28-31). Indeed, the block re-ordering done in Candelore uses an "address data signal" for scrambling.

The Examiner acknowledges that Candelore does not teach encrypting the table with a key. However, Candelore fails also to teach use of a key internal to the decoder to define a write order of data blocks, and to allocate corresponding sectors in a file allocation table. All three of these uses of a key are described in the specification (and claimed in claims 4 and 5), and the combination is not described or suggested in Candelore or in view of Sandstrom.

The Examiner has indicated that Sandstrom provides a teaching of encryption of the table showing the storage locations of the data blocks. However, Sandstrom discloses a method for securely storing electronic records. The context of Sandstrom is the need in business to be able to establish that a particular electronic record was created or existed at a particular time (col 1, lines 23-24), and in particular to provide an alternative to the prior art technique of using the hash of the particular record at the particular time (col 2, lines 1-3). The alternative provided by Sandstrom is to combine an identification code and time data of the electronic record from a trusted source to generate a key which is then used to encrypt a private area, associated with the electronic record, containing a verification code (col 2, lines 15-25). There does not appear in Sandstrom any disclosure or suggestion related to the encryption of a storage location table. The Examiner's citations do not support the contrary assertion made in the office action.

Consequently, the Examiner's acknowledgment that Candelore fails to teach encryption of the storage location table with a key is sufficient to remove Candelore as reference, with or without the combination of Sandstrom. This applies to independent claims 1, 14 and 25, and all the claims dependent therefrom, all of which contain the element of key encryption of a storage location table. This includes claim 10, making it unnecessary to consider the Mishina reference. The independent claims have been amended in order to clarify that the key is unique to the decoder.

In view of the foregoing, it is requested that the application be reconsidered, that claims 1-27 be allowed, and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at 703-787-9400 (fax: 703-787-7557; email: clyde@wcc-ip.com) to discuss any other changes deemed necessary in a telephonic or personal interview.

If an extension of time is required for this response to be considered as being timely filed, a conditional petition is hereby made for such extension of time. Please charge any deficiencies in fees and credit any overpayment of fees to Deposit Account 09-0457 (IBM-Endicott).

Respectfully submitted,

Clyde R Christofferson
Reg. No. 34,138

Whitham, Curtis & Christofferson, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA 20190
703-787-9400
703-787-7557 (fax)

Customer No. 30743